See Also: the University of British Columbia iSchool Student Journal
Vol. 3 (Spring 2017)

The preservation of digital signatures on the blockchain

Stephen Thompson

School of Library, Archival and Information Studies, UBC

s.thompson@alumni.ubc.ca

Keywords: digital signatures, blockchain, keys, encryption, authenticity, trust

Abstract

The blockchain is a distributed network that records digital transactions on a publicly accessible ledger. This paper explores whether blockchain technology is a suitable platform for the preservation of digital signatures and public/private key pairs. Conventional infrastructures use digital certificates, issued by certification authorities, to declare the authentication of key pairs and digital signatures. This paper suggests that the blockchain's hash functions offer a better strategy for signature preservation than digital certificates. Compared to digital certificates, hashing provides better privacy and security. It is a form of authentication that does not require trust in a third-party authority, and the distributed nature of the blockchain network removes the problem of a single point of failure. This article is an appendix to the research paper *Blockchain Technology for Recordkeeping* (Lemieux, 2016).

Introduction

The blockchain has been with us since 2009. In its seven years of existence, it has successfully resisted attempts to hack into it, take it down or co-opt it. While the technology is at a crossroads in its development, there are many use cases for its adoption across industry, including the field of records management.

The notarization of electronic records presents novel challenges for records managers. In a paper records environment, the creator of a record states ownership of the document, or assents to an agreement articulated in the document, by signing or countersigning it. From the records manager's perspective, the document is the property of the party that signed it. The signature is synonymous with the document.

In a digital records environment, we now have the "digital signature." The preservation of digital signatures is central to the concerns of the archivist. In this paper, I discuss the process of creating digital signatures. I review the advantages and limitations of public key infrastructures (PKIs), the established repository for the storage of the signatures. I compare PKIs with the architecture

around the blockchain's handling of the signatures. I conclude that the blockchain is a sounder platform for the preservation of digital signatures than the PKIs.

Defining "electronic" versus "digital"

Signatures generated on the blockchain are correctly referred to as "digital" rather than "electronic". Electronic signatures are an "electronic sound, symbol, or process attached to, or logically associated with, a contract or other record and…adopted by a person with the intent to sign the record" (Electronic Signatures in Global and National Commerce Act, §§ 106(b,5), 2000). In other words, it can be a scan of a handwritten signature or an image digitally "written" onto a screen that fulfils the same function as a handwritten signature. Digital signatures are a particular type of electronic signature that encrypt the signed document and help to authenticate its identity on subsequent occasions (Power, 2013). They are created in the digital environment to provide a layer of validation and transmission for public key encryption databases (Katz, 2010).

At the level of records, this digital-only approach is informed by the new Canadian General Standards Board (CGSB) standard on electronic records as documentary evidence. The standard distinguishes digital records from electronic records. Electronic records refer to any machine-readable record, whether it was created digitally or through analogue means. Digital records are those electronic records that consist of "discrete binary values aggregated into one or more bit stream" (CGSB 72.34-2015, 0.1).

It is through questions concerning the preservation of digital signatures that the blockchain enters the discussion. To understand the role of blockchain technology in the notarization of electronic records, it is instructive to examine the academic discourse on digital signatures and their preservation prior to the advent of the blockchain.

What are the characteristics of digital signatures?

Digital signatures are designed to guard against tampering and forgery in digital communications (Rouse, 2014).

There is agreement among records managers that authentication is the prime purpose of digital signatures (Boudrez, 2007, p. 180); Blanchette, 2006, p. 70 & 2012, p. 1). Methods and systems for the verification and authentication of electronic records are a topic of ongoing discussion.

Digital signatures have these key characteristics:

- They are based on *public-key cryptography* (Blanchette, 2006, p. 72).
- They are accepted as *legal evidence* (Blanchette, 2012, p. 1; Electronic Signatures in Global and National Commerce Act, §§ 101(g), 2000).
- They provide *authenticity* for a document during its transfer from one digital space to another (Blanchette, 2012, p. 5).
- Unlike written signatures, digital signatures do not prove the identity of the signatory. They provide authentication of the document's *bitstream,* in that the sender has

encrypted it with his public key and the receiver decrypts it with his private key (Boudrez, 2007, p. 183).

- Bitstream authentication supposes that *the individual and his private key are linked* (Blanchette, 2006, p.72 & 2012, p. 1; Boudrez, 2007, p. 184).
- They are *non-repudiable*. They not only preserve the integrity of the document but, state that the two contracting parties were the only counterparties and that only they could have produced their respective signatures (Blanchette, 2006, p. 72; CGI, 2004, p. 11; Buldas et al., p. 4).
- The cryptographic signatures mitigate any attempts to alter the *integrity* of a document after it has been signed (Blanchette, 2006, p. 73; Boudrez, 2007, p. 180; Lemieux, 2016).

How do digital signatures work?

To create a digital signature, counterparties sign the document directly. This structure differs from that of the blockchain, where the counterparties sign a hash that represents the document.

This paper will refer to asymmetric or "public key" cryptography, which involves an interaction between public and private keys. The public key is stored on a server accessible to other users on the network, while the private key remains a secret.

Public key cryptography operates under a dual procedure of which signatures form a part. Assuming there are two parties, each party possesses a key pair: the public and private keys. Figure 1 shows the following process: Alice and Bob are fellow archivists about to manage the transmission of a document. Alice is about to send a document to Bob across the network. Before she does so, Alice encrypts the document with Bob's public key. Alice sends it across, and Bob decrypts the file with his private key.

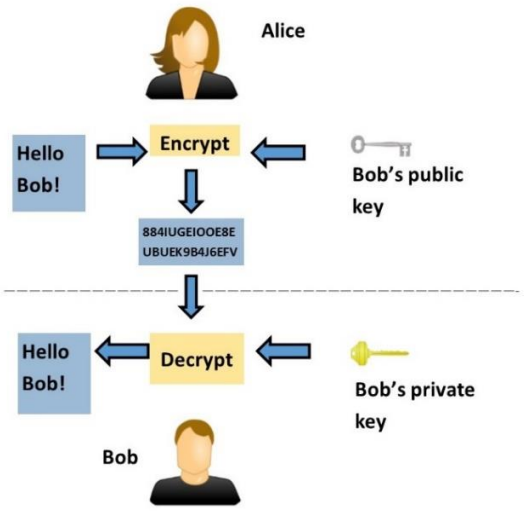

Fig.1 Public key encryption of a document

For the signature (Figure 2), the roles are reversed: Alice encrypts that same document with her private key and then sends it to Bob. Bob decrypts it with both his private key and Alice's public key. If he decrypts it successfully, Bob can then verify that Alice was the sender. The document, standing as a new file, should state that it has been verified. The resulting digital signature is intended to be available for anyone to verify the identity of the party that signed the document (in this case, Alice). The signature will be available not only to Bob, but to subsequent third parties as well. From the point-of-view of the archivist, the signature is *genuine* in that it is what it claims to be, and it is *authentic* in that the elements that are required for that authenticity are present (Duranti, 1989, p. 17).

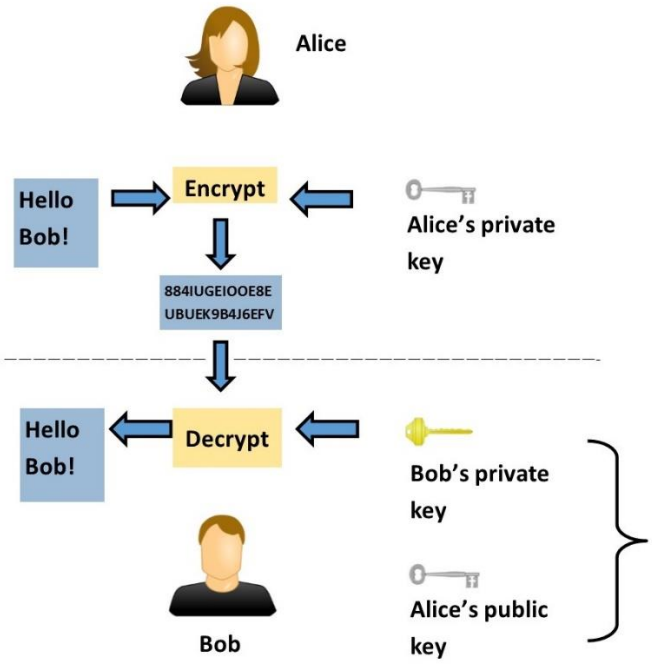

Fig.2 Public key encryption for the signature of a document

Hashing

Should Alice wish to speed up the process, she could create a cryptographic hash of the document and digitally sign the outputted hash value. In contrast to digital signatures, hashing is a form of document authentication in which documents are not signed directly. Instead, a hash function generates a hash value to confirm that the authentication of the digital signatures has taken place. There are two components to hashing:

- The *hash function* is a hexadecimal algorithm, such as SHA-256, that maps an input data of any size into a uniform, usually compressed, file size. In digital preservation, hash functions confirm that no changes have been made to a digital document (Van Garderen, 2016a).

- The *hash value* is the output of a specific length that permanently identifies the input data (Pedro, 2015, p.95).

The hash function is a one-way process. This means that the user can create the hash from input data, but not use the hash to reveal the data. Should a records manager alter even one bit from the input data and then try to apply the same hash function, the manager will generate a completely different hash value (Pedro, 2015, p. 97).

Applying these principles to the previous scenario, Alice authenticates the document not by signing it but by generating the hash value. The hash value is then broadcast to the network to confirm that the transfer of the document has taken place. Hash values have the following advantages:

- They can confirm the creation of content bundles such as datasets, degree certificates and ID management.
- They can authenticate that same document in the future, as long as it has not been altered (Lemieux, 2016).
- The hash is a smaller file size than the input data and so can be stored more easily (Pedro, 2015, p. 99).

Public key infrastructures (PKIs)

PKIs can come in the form of key management servers or centralized directories. They store key pairs, digital signatures, digital certificates and hash values. According to the CGI's 2004 white paper on public key encryption (p. 10-11), they combine software with a management process that covers the following operations:

- *The creation of the key pair* – Pedro (2015, p. 53) used the analogy of keys unlocking a safe. The private key unlocks the safe while the public key locks the safe. To decrypt Alice's document, Bob creates a private-public key pair by running a key generation algorithm from the PKI.
- *The creation of digital certificates* – certificates verify the digital signature by displaying the link between Alice and her public key. In those systems that issue certificates, the signature is known as a "qualified digital signature". They produce the validity period, the signature algorithm, a serial number and the name of the certification authority (Boudrez, 2007). These validity periods can be of a long duration and they also rely on the sustained readability and integrity of the signatures (Gladney, 2007, p. 170).
- *Private key protection* – in key pairings, the encrypted private key is mathematically linked to the public key, which is unencrypted (Pedro, 2015, p. 53). Despite this link, it is computationally infeasible to deduce the value of the private key from the value of the public key (Gladney, 2007, p. 168).
- *Certificate revocation in the event of a compromised private key* – once a user's certificate has been revoked, the PKI must preserve the certificate on a database accessible to all

users in the network so that it cannot be re-used. This addresses a problem identified by Kohnfelder (1978, p. 16): a public file encryption function has a single point of failure. Once breached, the attacker can pass encryption functions that are bogus. Kohnfelder also stated that updating such a large system would be expensive and inefficient.

- *Private key backup and recovery* – if the user loses his private key, any files encrypted with that key will be lost. The PKI needs a backup and recovery mechanism for lost private keys.
- *Key and certificate update* – this is a mechanism for the renewal of expiring digital certificates. The PKI achieves this by carrying out the renewal automatically or notifying the user to carry out an operation that updates the certificate himself. Blanchette (2012, p. 77) stated that the idea behind fixed expiry dates is to mitigate against incremental damage to the network's integrity due to corrupted public keys.
- *Key history management* – following a key update that generates new key pairs, history management makes it easier for the user to determine which private key to use for decrypting files.
- *Certificate access* – the 2004 CGI white paper suggested a Lightweight Directory Access Protocol (LDAP) directory for convenient access to certificates.

PKIs therefore require the preservation of at least three components: key pairs, active digital certificates and revoked digital certificates.

Certification Authorities: The trusted third party

Trusted third parties (TTPs) have been defined as a "secure middle layer on (cloud) service transactions" (Stamou et al., 2013, p. 4976). They allow the secure, trustful, interaction between two parties (ibid., p. 4979). TTPs can be public sector organizations, such as the NSA and GCHQ, or they can originate from the private sector, e.g. GlobalSign, Symantec and Comodo.

Certification Authorities (CAs) are a type of TTP that deliver validation authority for a PKI (Black & Layton, p. 13, 2014). PKIs assume the presence of CAs. Users of the network store their public key with the CA, which they recognise as a trusted third party that can vouchsafe the public key on its server. CAs verify the identity of each user and sign their public keys. In Alice and Bob's exchange of signatures, Alice is presenting her CA certificate, with the signature and public key both embedded, to Bob (Pedro, 2014, p. 55).

Caveats with digital signatures on PKIs

TTPs as a central point of failure

Users store their signatures with a TTP because they trust the integrity of the organization, but TPPs operate under minimal legal enforcement. Further, because most TPPs are centralized, they stand as a "central point of failure" (Allen et al., 2015, p. 2). The risks of storing signatures on a centralized platform owned by an organization include:

- Ownership of key pairs becomes ambiguous once entrusted to a TTP (Allen et al., 2015, p. 2).
- TPPs are not bound to conform with national or international legislation (Stamou et al., 2012, p. 4981).
- TPPs are not obliged to enforce their own security policies (ibid.)
- It is difficult to control the internal governance of a TTP and to compel them to offer external ports in their systems or to submit accurate logs on a user's request (ibid.)

Digital signatures validate and sign the bitstream of a document, not the document itself (OCLC/RLG Working Group, 2002; Boudrez, 2007, p. 183)

As an example, a *fonds* contains a video of an event in the 'wmv' format but the archivist converts it to an 'mp4' so that it will be viewable across a wider range of platforms. The signature verifies the bitstream of the 'wmv'. However, should the archivist believe that the *content* of the video had been digitally signed and attempt to authenticate the 'mp4' with the same signature that had come with the 'wmv' file, the authentication will fail.

Verification is not protection

The digital signature does not prove the integrity of the digital record. It only proves whether the digital document had been altered post-verification; it does not prevent the alteration from taking place. This is why encryption is required when using digital signatures. Also, it only verifies a document at the point of transfer and not at any time thereafter (Boudrez, 2007, p. 183, citing National Archives Australia).

New signatures required for file conversions

With each data migration or file format conversion, a digital archivist will need to generate a new set of signatures to authenticate the digital transfer. The dilemma this creates for the archivist is whether to preserve only the originating signature set or to archive them as a validation chain in a parallel repository that can capture future signatures generated over time (Boudrez, 2007, p. 186-7). And, should the archivist decide to archive them, would he build it internally or would he migrate them to an external server? If he enacts the former solution, he will create an extra layer of digital archiving but would maintain control over the signatures. If he enacts the latter, he can upload them to a PKI solution but lose direct control.

How does the blockchain preserve documents?

Peter Van Garderen, the developer of the Archivematica and AtoM digital archiving systems, defines the blockchain as "an immutable chain of data" that stores grouped transactions into timestamped blocks (Van Garderen, 2016a). The main archiving strength of the blockchain is that hash values generated will be preserved on the blockchain for as long as the blockchain continues to operate.

The blockchain is a type of distributed PKI. There are major differences between the purpose and application of signatures in a conventional, centralized, PKI and the purpose and application of signatures in the blockchain. In a conventional PKI, the hash value is used for the authentication of the digital certificate. In the blockchain, the hash value authenticates both transaction data and block data. Additionally, hash values in the blockchain can be stored privately and separately from the application that generated the hash value (Pedro, 2015, p. 99).

Proof-of-work

Proof-of-work is the algorithm that ensures the security and transparency of the Bitcoin blockchain. It runs on SHA-256 hash functions. Full nodes, known as miners, authenticate 10 minutes' worth of Bitcoin blockchain transactions into a block by solving a mathematical puzzle that generates a hash value for that block. In doing so, the miner has successfully "mined" the block and proved to the network that he has exerted the work required to hash the block. In return, the network rewards the miner with a fixed quantity of bitcoins. Hashing is a key feature of proof-of-work (Pedro, 2015, p. 96).

Proof-of-work operates on the same principle as a CAPTCHA where the prospective user must pass a test in order to access a service (Pedro, 2015, p. 102). Proof-of-work utilises the blockchain's computational power against attempts to tamper with the blocks (ibid., p. 95). Proof-of-work relates to the main principle of hashing. In our Alice and Bob transfer, the hashing is a proof-of-work that the document has been authenticated.

Proof-of-stake

This Ethereum blockchain is a decentralized super-computer that runs smart contracts and other decentralized apps (Ethereum Project, 2017). Proof-of-stake is the principal property of Ethereum. Participants in this blockchain purchase tokens that enable them to transact in auctions, prediction markets and in events that require decision making, such as the future of the network. They do this by proving that their balance is sufficient to participate. The users prove their commitment to a transaction by "minting" (i.e., publishing), blocks in proportion to the quantity of tokens they hold, as opposed to mining them. This is more environmentally friendly than the proof-of-work function, because it does not require nearly as much computational power as mining. Other advantages of proof-of-stake are that the activity is open to all stakeholders on the network and, because of the lower computational power required, the transaction fees are lower (Pedro, 2015, p. 235).

There is disagreement, however, about the risk of centralization. Pedro (2015) argued that as there is wider participation among the users, proof-of-stake is less susceptible to centralization. Bentov et al. (2014, p. 34) countered that proof-of-stake would place amateur minters in a conflict of interest against professionalized miners. Bentov (2014) expected the miners to prevail and then make centralizing moves to consolidate their control over the network.

Proof-of-concept

In the context of the blockchain, proof-of-concept is the creation of a digital sandbox within which the entrepreneur can build a solution, gather supporting datasets, then hash the sets and

broadcast them to the blockchain (Troy, 2016). This system does not impact on the owners of the datasets, even though the datasets themselves may be real.

In the context of digital preservation, cryptographic hash functions are used to produce proof of a digital action that is unique, meaning that there is no identical hash (Van Garderen, 2016b). The identifier for the hash value of a proof-of-concept will be unique.

Specialized signatures

The blockchain community has conceived an array of signatures that utilise the hashing process in a way that can solve various issues, mainly concerning space. Two of these are of particular relevance in records management:

- *Elliptic Curve Digital Signature Algorithm (ECDSA)* – ECDSA combines elliptic curves (a public key family) with the DSA digital signature, which together form the signature scheme used in Bitcoin (Pedro, 2015, p. 70). The feature that would be of interest to an archivist looking for an efficient preservation strategy is that there is no need to store the public key, as it can be hashed repeatedly in the future (Lemieux, 2016).
- *Schnorr signatures* - this is an overriding signature that hashes a cluster of signatures that remedy file storage issues. For example, if a *fonds* contains thirty documents each with their own signature, the archivist can sign the entire *fonds* with a Schnorr signature. He would reduce the file size from 2400 bytes (80 bytes per signature) back to 80 bytes. The cryptography community approves of Schnorr signatures because of their speed, simplicity and strong security (van Wirdum, 2016, para. 14; Allen, 2015, para. 3). Some in the Bitcoin community have called for them to become the standard (Pedro, 2015, p. 58). For the archivist, these signatures provide a simple means of preserving new *fonds* that contain a large number of documents.

Timestamping

A timestamp proves that a certain dataset existed at a certain point in time (Pedro, 2015, p. 99). The blockchain method creates timestamped blocks through peer-to-peer technology, therefore disintermediating Time Stamping Authorities (TSAs). Miners on the Bitcoin blockchain timestamp each block which contains ten minutes' worth of transactions. The miners are, effectively, operating as a distributed TSA. This means that there is no need for periodic re-timestamping of signatures due to expiring keys. In promotional materials for its new BLT cryptographic algorithm, the software security company Guardtime stated the time and integrity of the signature can be proven mathematically, without reliance on the security of keys or of trusted parties (Guardtime, 2016).

Amanti (2016) stated that the time it takes for a TSA to verify a transfer is measured in seconds, whereas the blockchain's verification takes minutes (para. 23). He also noted two other advantages of blockchain timestamping over TSA timestamping:

- Long-term preservation can be achieved without the maintenance costs that come with a TSA-issued certificate (Amati, 2016, para. 24).

- Archivists can exploit the convenience of verifying the signature with the document and public key without having to safeguard the digital signature on a central server (Amati, 2016, para. 25).

Can blockchain technology meet existing preservation standards?

ISO 18492:2005 - Long-term preservation of electronic document-based information

The chief provision of ISO 18492:2005 is to guide information professionals on the long-term preservation and retrieval of authentic information on document-based systems. The standard articulates the dilemma faced by digital records managers as they consider the option to use blockchain technology alongside their existing systems. It indirectly offers strategies for a blockchain system to preserve and retrieve metadata about documents, such as the signatures.

An important innovation that the blockchain offers that meets the standard is the creation of hash values, independently of file format. I will discuss this further in my analysis of ISO 15489-1 and of file formats.

ISO 14721:2012 (OAIS – Open Archival Information Systems)

This standard defines the OAIS model as a system that preserves archival information on a publicly-accessible channel. I would like to focus on one element of the model: the authentication process for the Content Data Objects. Records managers place importance on protecting the authenticity of their records for the longer term (Lemieux, 2016, p. 5, 10). The recommended authentication process as stated in ISO 14721:2012 acknowledges this by requiring the authentication of the document to be repeatable (OCLC/RLG Working Group, 2002, p. 44).

There are four types of Preservation Description information in the OAIS model (figure 3). Blockchain metadata can be applied to this information in the following ways:

1) Provenance – any adjustment in the bitstream of a document requires a new hash value for the document to continue to reconcile with the corresponding identifiers in the blockchain. A library can utilize this property of the blockchain to maintain a record of the digital transitions of that document.
2) Context – Because the blockchain is not concerned with the circumstances behind a document's creation, it is not applicable to this type of information.
3) Reference – The hash value identifies the bitstream of a document at a certain point in time.
4) Fixity – The blockchain is, at the time of writing, immutable.

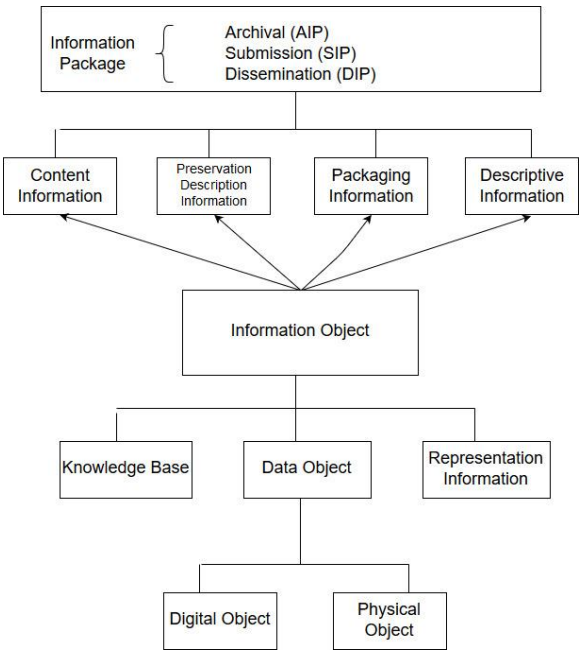

Fig 3. OAIS Information Model. Copyright 2002 OCLC Online Computer Library Center, Inc. 6565 Frantz Road, Dublin, Ohio 43017-3395 USA http://www.oclc.org/

ISO 15489-1:2016 – Management and control of records with their metadata

This standard sets out rules for the long-term management and control of records and their metadata, regardless of their structure or format. Referring to the previous 2001 standard, Lemieux (2016) described the standard as recommending the retention of the history of a record so that future users can judge its reliability (Lemieux, 2016, p. 4) and its authenticity (ibid., p. 5).

When a transaction is made on the blockchain, the document is separated from its hash metadata, i.e. keys and signatures. The document remains on the archive's database but the hash metadata migrates to the blockchain database. This blockchain metadata is accessible on https://blockchain.info. Any visitor can view the hash value of a block and all the transactions that took place therein. Click here for an example. When they view downloaded blocks (for those who download the blockchain), they will see that there is no blockchain file format either for the blocks, the keys or the signatures.

This element of the blockchain database makes it easier to comply with ISO 15489 by using metadata formats, such as 'dat', which are not reliant on any document type. However, Van Garderen has stated that the blockchain community is incorrect in believing that placing records on the blockchain solves the issues stated in section 5.2.2 of the standard, surrounding authenticity, reliability, integrity and usability of records. At his presentation at Simon Fraser University in May 2016, he stated that he would not be confident selling the blockchain as a universal panacea for all records management problems (Van Garderen, 2016b).

RFC 3161 / ANSI X9.95 – timestamping

Existing standards, such as RFC 3161 and ANSI X9.95, require trusted third parties, or digital notaries (Pedro, 2015, p. 100), to administer timestamps. These parties are known as Time Stamping Authorities (TSAs). RFC 3161 sets out the respective formats for which TSAs receive requests for a timestamp and the TSAs' response (RFC 3161).

ANSI X9.95 also deals with time stamping of documents, but with an emphasis on the security of financial transactions (ANSI, 2012).

RFC 3161 defines a timestamping service as a proof mechanism "that a datum existed before a particular time". The point behind this mechanism is to enable the archivist to verify that any digital signatures, coming under the archivist's jurisdiction in a *fonds*, had been created within the validity date of the public key certificate (RFC 3161, 2001).

Amati (2016) recognised that their long-term preservation requires management in order to maintain the certified timestamp's validity: this management would involve renovation of the signatures, timestamp chaining and certificates (para. 22).

Comparisons between the blockchain and PKIs

I have discussed how PKIs combine digital certificate administration with key management. The preservation of digital signatures on the blockchain network has a different architecture and a different purpose. It has been argued (e.g., Lemieux, 2016) that the blockchain is gradually becoming recognized as a viable solution for the professional need for trusted digital records and public registration systems in general.

> ***Certification*** – The Bitcoin blockchain is a PKI that neither issues digital certificates nor operates through a CA. Blockchain technology does not require a digital certificate for its users to trust the integrity of the network because the blockchain miners have already verified the transfer of digital value.
>
> ***Decentralization*** – returning to the point about PKIs and the potentially serious issue of the 'single point of failure', the server room or the cloud can be seen as the 'single point of failure' that Kohnfelder was alluding to. The main advantage that a digital signature database on the blockchain network has over databases on centralized systems is the act of distributing a blockchain-based PKI infrastructure across a range of computers, or nodes. This decentralized structure enhances the longevity of the network because duplicates of the blocks, on which the signatures are stored, are so numerous (Findlay, 2015, para. 22). The decentralization of the blockchain gives it a further advantage in that no third party can alter or erase the transactions stored in the blocks without undoing the proof-of-work requirement that had verified them (Findlay, 2015, para. 13).
>
> ***Distributed consensus*** – thousands of computers located around the world, known as 'nodes', verify each transaction by authenticating the digital signatures *en masse*: they reach consensus about the integrity of each transaction. This process is an element of the decentralized nature of the blockchain and some have argued that it gives the blockchain

more integrity than authentication by a single CA (Lea, 2016). Amati (2016) stated three complementary positives of the blockchain's consensus on signatures:

- All agree on the latest signatures.
- We are seeing the same signatures.
- No-one can alter the signatures (para. 30).

Instead of relying on a central authority to certify a document's authenticity, the blockchain can assert proof of its authenticity through cryptographic confirmation. This dynamic can empower many archive managers to establish their own records systems backed by the assurance and longevity of the distributed blockchain network (Findlay, 2015, para. 14).

Notarization – a notary is a trusted authority that verifies or authenticates a transaction and the users in the network place trust in that notary that it will store, securely, the data in question (Economist, 2015, para. 7). A CA is a type of notary for key pairs. In the blockchain, a distributed consensus on the blockchain can take on notarial operations from trusted authorities (Li, 2016, para. 11).

Privacy – the encryption in the blockchain's distributed network offers strong security and privacy when verifying signatures. The way privacy differs on the blockchain from that of a PKI is that despite the public nature of the transactions and value balances, the counterparties behind the transactions remain private (Pedro, ch.13, p. 209). The blockchain record will say that Bitcoin address *x* sent a specified amount of digital value to Bitcoin address *y*. However, the more frequently they use the same Bitcoin addresses for future transactions, the further their privacy erodes. For example, an agent will be able to establish relationships between Bitcoin addresses. So, the question of privacy on the blockchain depends on the diligence of the counterparties to create new addresses per transaction. Pedro's chapter 13 (pp. 209-229) offers a full discussion about the privacy issue.

Independent of file format – a digital archive should ensure that its authentication system is file format neutral. This reduces the problem of relying on applications that transfer data, proprietary or open-source, becoming obsolete (Findlay, 2005, para. 13).

Conclusion

This paper has assessed public key infrastructures and surveyed the features of the Bitcoin blockchain. The answer to the question as to whether a blockchain-powered PKI offers better signature preservation strategies than CA-controlled PKIs depends on what metadata the information professional selects for archival storage and the duration of the retention/disposition schedule. Boudrez (2007) stated that records of the validation metadata can replace that of the digital signature for those digitally-signed records which have a permanent retention period (p. 190). Therefore, blockchain adoption may be more advantageous to records with a permanent retention schedule. This is because the hash value, a feature of the blockchain, stands as validation metadata that would not require specific software for its future verification. Furthermore, the blockchain record does not require a centralized party, such as a CA, to notarize

or validate the hashes – unless the records management utilises sidechains and third-party notaries such as Factum.

Developments in the Ethereum blockchain offer a point of entry for the information professions at a lower cost than the Bitcoin blockchain. The proof-of-stake versus proof-of-work conflict will have a different outcome for decentralized networks. In the case of a large blockchain network such as Bitcoin, where hashing power for block creation requires the corporatization of miners, Bentov's scenario of proof-of-work dominating the network is most likely to play out. However, in emerging, decentralized blockchains such as Ethereum, where mining is still accessible to the user community, Pedro's optimism for the benefits of proof-of-stake can hold.

Blockchain technology is in a transitional phase. This July (2016) alone has seen the halving in the Bitcoin blockchain and the hard fork on that of Ethereum. The blockchain community has yet to see the ramifications of these developments play out. The blockchain offers exciting options for the library, archival and records management communities, but information professionals would be wise to wait before adopting these technologies.

References

Allen, C. (2015, October 9). Schnorr signatures: An overview. *WebOfTrustInfo*. Retrieved from https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/topics-and-advance-readings/Schnorr-Signatures--An-Overview.md.

Allen, C., Brock, A., Buterin, V., Callas, J., Dorje, D., Lundkvist, C., Kravchenko, P., Nelson, J., Reed, D., Sabadello, M., Slepak, G., Thorp, N. & Wood, H. T. (2015). *Decentralized public key infrastructure. A White Paper from Rebooting the Web of Trust*. Retrieved from https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/final-documents/dpki.pdf

Amati, F. (2016, January). Using the blockchain as a digital signature scheme. Medium blog. Retrieved from https://blog.signatura.co/using-the-blockchain-as-a-digital-signature-scheme-f584278ae826

Anon. (2015, October 31). The trust machine: The promise of the blockchain. *The Economist*. Retrieved from http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

ANSI X9.95-2012. Trusted time stamp management and security. Retrieved from https://www.sec.gov/rules/proposed/s72703/iac120105.pdf.

Bentov, I., Lee, C., Rosenfeld, M. & Mizrahi, A. (2014). Proof of activity: Extending Bitcoin's proof-of-work via proof-of-stake. [Extended Abstract] *Performance Evaluation Review*, 42 93), 34-37.

Bitcointalk.org. Retrieved from https://bitcointalk.org/index.php?topic=101514.0

Black, P. & Layton, R. (2014). *Be careful who you trust: Issues with the Public Key Infrastructure*. 2014 Fifth Cybercrime and Trustworthy Computing Conference. IEEE Computer Society. Retrieved from https://www.researchgate.net/publication/282936649_Be_careful_who_you_trust_Issues_wit

h the public key infrastructure

Blanchette, Jean-François. (2012). *Burdens of proof: Cryptographic culture and evidence law in the age of electronic documents*. Cambridge: The MIT Press.

Blanchette, Jean-François. (2006). The digital signature dilemma. *Annales des Telecommunications*, 61(7), pp. 908-923.

Blockchain.info. Retrieved from https://blockchain.info.

BlockNotary. Retrieved from https://www.blocknotary.com/

Boudrez, F. (2007). Digital signatures and electronic records. *Archival Science*, 7(2), pp. 179-193.

Buldas, A., Laanoja, R. & Truu, A. (2014). *Efficient implementation of keyless signatures with hash sequence authentication*. [Unpublished paper.] Retrieved from https://eprint.iacr.org/2014/689.pdf.

CGI (2004). *Public key encryption and digital signature: How do they work?* White Paper. Retrieved from www.cgi.com/files/white-papers/cgi_whpr_35_pki_e.pdf.

Clanchy, M. T. (2013). *From memory to written record: England 1066-1307*. Chichester, John Wiley & Sons Ltd.

CGSB 72.34-2015, 0.1. Electronic records as documentary evidence. Personal communication of draft by e-mail.

Cumming, K. & Findlay, C. (2016). Report on blockchain: Applications and implications. *Recordkeeping Roundtable*. Retrieved from https://rkroundtable.org/2016/04/03/report-on-blockchain-applications-and-implications/.

Curry, I. (2001, March). An introduction to cryptography and digital signatures. Entrust. Retrieved from https://www.entrust.com/wp-content/uploads/2013/05/cryptointro.pdf

Duranti, L. (1989). Diplomatics: New uses for an old science. *Archivaria*, 28, pp. 17-27.

Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 7006 (2000). Web: https://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf

Ethereum Project (2017). Retrieved from https://ethereum.org

Findlay, C. (2015). Decentralised and inviolate: the blockchain and digital archives. Retrieved from https://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/.

Van Garderen, P. (2016, May 17). Blockchain and digital preservation – Part2. Presentation at Simon Fraser University [Video file]. Retrieved from https://www.youtube.com/watch?v=S2N0m9YDgZw.

Van Garderen, P. (2016, May 17). Blockchain and digital preservation – Part3. Presentation at Simon Fraser University [Video file]. Retrieved from https://www.youtube.com/watch?v=onx3f6xmEsI&t=276s.

Gladney, H. (2007). *Preserving digital information*. Berlin, Heidelberg: Springer.

Guardtime. Retrieved from https://guardtime.com/blt-technology.

ISO 16363:2012. Space data and information transfer systems – Audit and certification of trustworthy digital repositories. Geneva: ISO. Retrieved from http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62542.

ISO 15489-1:2016. Information and documentation – Records management – Part 1: Concepts and principles. Geneva: ISO. Retrieved from http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62542.

ISO/TR 18492:2005. Long-term preservation of electronic document-based information. Geneva: ISO. Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38716.

Katz, J. (2008). Digital signatures. Berlin, Heidelberg: Springer.

Kohnfelder, L. (1978). *Towards a practical public key cryptosystem.* Bachelor's degree thesis. Retrieved from http://groups.csail.mit.edu/cis/theses/kohnfelder-bs.pdf.

Lea, T. (2016). Introductory course – The power of the blockchain. What is blockchain? Retrieved from https://www.youtube.com/watch?v=KXC9hyB09pk

Lemieux, V. (2016). Blockchain technology for recordkeeping: Help or hype? Retrieved from http://www.blockchainubc.ca/main/dissemination

Lemieux, V. (2016). Trusting records: Is blockchain technology the answer? *Records Management Journal*, 26(2), pp. TBA.

Li, V. (2016, March). Bitcoin's useful backbone: Blockchain technology gains use in business, finance and contracts. *ABA Journal*, 102(3), p.31. Retrieved from http://www.abajournal.com/magazine/article/bitcoins_underlying_technology_blockchain_gains_use_in_business_finance_and

OCLC/RLG Working Group. (2002, June). *Preservation metadata and the OAIS Information Model: A metadata framework to support the preservation of digital objects*. Retrieved from http://www.oclc.org/content/dam/research/activities/pmwg/pm_framework.pdf.

Pedro, F. (2015). *Understanding Bitcoin: Cryptography, engineering and economics*. Chichester: John Wiley & Sons Ltd.

Power, M.E. (2013). *The difference between e-signatures and digital signatures*. eSignLive.com. Retrieved from: https://www.esignlive.com/blog/the-difference-between-e-signatures-and-digital-signatures/

RFC 3161. (2001, August). Internet X.509 public key infrastructure time-stamp protocol (TSP). Retrieved from http://www.rfc-base.org/txt/rfc-3161.txt.

Rouse, M. (2014). Digital signature. *SearchSecurity.TechTarget*. Retrieved from http://searchsecurity.techtarget.com/definition/digital-signature.

Ruggieri, F. (2014). Security in digital data preservation. *Digital Evidence and Electronic Signature Law Review*, 11, pp. 100-106.

Stamou, K., Aubert, J., Gateau, B., Morin, J-H. (2012). *Preliminary requirements on trusted third parties for service transactions in cloud environments*. 2013 46th Hawaii International Conference on System Sciences. Institute of Electrical and Electronics Engineers, 4976-4983.

Troy, S. (2016). Proof of concept for blockchain implementation necessary and tricky. *TechTarget*. Retrieved from http://searchcio.techtarget.com/feature/Proof-of-concept-for-blockchain-implementation-necessary-and-tricky.

Wirdum, A. van. (2016, April 14). The power of Schnorr: The signature algorithm to increase Bitcoin's scale and privacy. *Bitcoin Magazine*. Retrieved from https://bitcoinmagazine.com/articles/the-power-of-schnorr-the-signature-algorithm-to-increase-bitcoin-s-scale-and-privacy-1460642496

Stephen Thompson is a graduate student at the School of Library, Archival and Information Studies on the MLIS program. His research interests are technology, information security and scholarly communication. He is currently collaborating with Vicki Lemieux to launch a new blockchain knowledge platform, Blockchainubc.ca, that will investigate the applicability of blockchain technology to processes in records management, librarianship and archiving.